Accellion Share Securely™

AN ACCELLION WHITE PAPER

Accellion Security FAQ

Accellion, Inc.
1804 Embarcadero Road
Suite 200
Palo Alto, CA 94303

Tel +1 650 485-4300
Fax +1 650 485-4308
www.accellion.com
info@accellion.com

WP-ASFAQ-0911

Executive Summary

The world's leading corporations and government agencies rely on Accellion Secure File Transfer and Accellion Secure Collaboration to secure their intellectual property and ensure compliance. Accellion provides enterprise-class secure file sharing solutions for security and data leak prevention that meet today's business requirements for digital information sharing. Accellion is the pioneer and leading provider of integrated on-premise and off-premise file sharing solutions that span virtual and cloud environments.

This document answers frequently asked questions regarding the security features of the Accellion Secure File Transfer and Accellion Secure Collaboration solutions and their deployment as a virtual, physical or cloud appliance or Hosted Cloud Service.

Accellion Security Measures

AUTHENTICATION

Can I control who is authorized to use the Accellion system?

Yes, administrators can use the following methods of authentication control:

- Accellion supports integration with Internal directory systems such as LDAP (Lightweight Directory Access Protocol) and Active Directory and also LDAPS for the Hosted Cloud Service.
- Accellion supports single sign-on through SAML.
- The Accellion administrator can create multiple administrators for an Accellion Secure File Transfer or Accellion Secure Collaboration. Each administrator can be given permission to administer certain parts of the configuration.

How is authentication secured?

Accellion employs several layers of authentication to ensure that only authorized recipients can access the files:

- SECURE LINK/URL: Generated by a double 128-bit MD5 token -- 2^128 combinations are nearly impossible to guess.
- QUALIFIED LINK/URL: The link has a limited lifespan (configurable by the System Administrator to conform to company policy) and blocks access to the file after its expiration.
- CHALLENGE/RESPONSE: Before download, the users must identify themselves. When LDAP is deployed, Accellion will link this feature to the customer's LDAP directories.
- RECIPIENT VALIDATION: Accellion can verify if a user is on the original recipient list of the email for downloading a file. This prevents forwarding links. This is a System Administrators configurable option.
- RECIPIENT TRACKING: Logging of Recipient email address, time of access and IP address makes it easy to monitor suspicious activity.

  Recipients download the attachment via and HTTPS/SSL connection.

NETWORK/FIREWALL

How do I position the Accellion system for maximum security with external recipients? *(Applies to physical and virtual appliance)*

The Accellion system can work in a closed network if the solution is intended only for internal users. However, since file sharing is usually not limited to internal users, the Accellion system is typically deployed in a DMZ. The Accellion system is designed from the ground up with security as a primary concern. The

system functions with the encrypted traffic on SSL and IP sec ports only and it can also be made accessible to external users via a pass-through proxy.

How do I configure the Accellion system within my firewall?

The Accellion system is designed to work within firewalls. Accellion provides a deployment guide with the necessary information and detail to configure your firewall for optimal usability and security for your system. All traffic from the Accellion system is secure and encrypted. Communication within the system is over Ipsec. File uploads and downloads are via SSL.

TRANSPORT

How is secure transport of attachments achieved?

Transport security is based on these industry standard protocols:

• SECURE SOCKET LAYER/TRANSPORT LAYER SECURITY (SSL/TLS) http://www.ietf.org/rfc/rfc2246.txt: by which attachments are uploaded from senders and downloaded by recipients using HTTPS.

• IPSEC http://www.ietf.org/html.charters/ipsec-charter.html; by which files are replicated within the system from one appliance to another. (Replication can also occur over an organization's own secure VPN)

These protocols are best-of-breed, widely deployed and heavily-tested − and they offer state-of-the-art cryptography protection.

Are files secure when delivered from sender to recipient?

Yes, the Accellion system secures files in the following ways:

- The link/URL that is generated is constructed in a secure fashion − it is comprised of the following components that are encrypted into a one-way MD5 token (patent pending):
    - Shared Key - which establishes authentication
    - Link Expiry - which dictates the duration of the link/URL
    - File Name
- All file transfers are sent through SSL encrypted tunnels
- Files can be automatically encrypted with a unique key using AES 128
- Recipients download the file via an HTTPS/SSL connection

ENCRYPTION

If someone breaks into the system, will they have access to all of the files?

Accellion's restricted access protocols guard against malicious access:

- File names are de-referenced when stored on the appliance's hard drive to ensure that files are inaccessible.
- Files may be stored encrypted for added security.

- Data can be accessed only through the file URL embedded in the email.
- Each URL call is authenticated individually.
    - Access through SSH can be turned off by the administrator of the system.

How are files encrypted?

Files are encrypted using AES 128-bit encryption. (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf) Additionally each file is encrypted with a different unique key. That makes the system very secure and makes most attack methodologies ineffective since they have to start afresh for each file. The file encryption key is also not stored on the server, so even if the server is compromised, the decryption keys for stored files cannot be obtained on the server itself. All cryptographic libraries used are FIPs compliant and are the same as used in the FIPS certified version of the Accellion Secure File Transfer or Accellion Secure Collaboration.

Do administrators have access to the files?

Administrators do not have access to files once they are uploaded to the Accellion system. However, they can view the list of files and delete, replicate and set life cycle rules on these files. Administrators can also view reports and logs in relation to file access events.

ADMINISTRATION

How does the Accellion system track recipient download of attachments?

The Accellion system provides tracking at both the user and administrator level:

- USER LEVEL: return receipts to the sender specify which file has been downloaded, by whom (if recipient registration is required) and when.
- ADMINISTRATOR LEVEL: reports account for each and every access to a file, which affords a comprehensive audit trail and high visibility into the system − this feature can also serve to identify potential problem areas.

How does the Accellion system ensure that software updates are validated?

The Accellion system uses the following methodology to validate software updates:

- The update server is coded in the digitally signed license file.
- The update server uses token based authentication to validate the incoming calls to the server from the Accellion appliances.
- All updates are only over SSL.

With Accellion deployments on the later operating systems, the update packages are also signed using a public/private key and the appliance will validate the update package before applying it. (Note: this facility is only available on install.)

SECURITY & COMPLIANCE

Is Accellion FIPS 140-2 Certified?

Yes, the Accellion system is FIPS 140-2 certified. Accellion offers FIPS 140-2 compliance secure file sharing solutions for both on and off premise Cloud, Virtual and Hosted deployments.

Is Accellion Secure File Transfer and Accellion Secure Collaboration HIPAA/SOX/PCI compliant??

The Accellion Secure File Transfer and Accellion Secure Collaboration are FIPS 140-2 certified providing the necessary security and encryption technologies to meet HIPAA 2.0 compliance requirements. The Accellion application satisfies the "secure transmission" requirement by providing all communication (login sessions by users and admins, uploads and downloads) over HTTPS/SSL and providing an audit trail of all transactions. The administrator can view the following information of an audit trail: - Sender/Recipient email address - File name - Time and Date of the upload/download - File Size - Source IP address advertised by the sender/recipient.

Sarbanes-Oxley requires that business processes are auditable. Accellion provides its customers with the security, tracking and reporting tools necessary to demonstrate compliance.

Accellion provides PCI compliance by providing absolutely no access to a user's files in the Accellion system. Files are stored de-referenced from their file name, encrypted, and are not accessible by anyone – including Accellion support personnel. In order to access a file, you need to provide decryption information that is bundled into the link that is sent to the recipient.

How does Accellion create a hardened secure environment?

The Accellion Operating System is Enterprise Linux - CentOS 5.1

- Accellion appliances are based on a customized version of CentOS Ver5.1.
- Accellion allows for the administrator to shut down all SSH access to the machine.

Web Service (TCP Port 80 and 443)

- Apache 1.3.41
- Port 80 HTTP only enabled to redirect to SSL Port 443. All data and user access required over SSL through secured cookies and session IDs
- SSLProtocol TLSv1 and SSLv3 enabled all others disabled

Accellion Hosted Cloud Service

The Accellion Hosted Cloud Service extends Accellion Secure File Transfer and Accellion Secure Collaboration into the cloud, enabling highly scalable, elastic deployments of managed file security. The service provides organizations with the ability to rapidly implement secure file sharing to fix network security deficiencies, alleviate overloaded email systems, manage peaks in usage, and collaborate across the DMZ.

Accellion utilizes the Amazon Web Services AWS Cloud Computing Platform to deliver secure file sharing capabilities in the Cloud. This section answers frequently asked questions regarding the security of the Accellion Hosted Cloud Service running on AWS.

What certification does Amazon have?

Amazon Web Services' controls are evaluated every six months by an independent auditor in accordance with the Statement on Auditing Standards No. 70 (SAS70) Type II audit procedures.

PHYSICAL SECURITY

What physical security measures have been undertaken to protect AWS data centers?

AWS datacenters are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides datacenter access and information to employees and contractors who have a legitimate business need for such privileges.

How many dedicated information security personnel does Amazon Web Services have on staff?

This information is not provided as its misuse creates additional vulnerability to their facilities.

DATA INTEGRITY AND PROTECTION

Will Amazon Web Services or Accellion have access to a company's proprietary information?

No, AWS does not exercise access to customer data. AWS only provides datacenter access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to datacenters by AWS employees is logged and audited routinely.

Accellion provides absolutely no access to a user's files in the Accellion system. Files are stored de-referenced from their file name, encrypted, and are not accessible by anyone – including an Accellion support person. In order to access a file, you need to provide decryption information that is bundled into the link that is sent to the recipient. Customers can further ensure such by utilization of encryption and by shutting off access through SSH.

BUSINESS CONTINUITY MANAGEMENT

What process has Amazon put in place to ensure "continuous availability" of data?

The AWS data centers are designed to anticipate and tolerate failure while maintaining service levels. Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold."

In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration. In the event of a data center failure, there is sufficient capacity for the remaining sites to serve the load.

Customers should architect their AWS usage to take advantage of regions and Availability Zones. Distributing applications across multiple Availability Zones provides the ability to remain resilient in the face of most failure modes including natural disasters or system failures.

How rapidly does AWS respond to incidents?

The Amazon Incident Management team employs industry-standard diagnosis procedures to drive resolution during business impacting events. Staff operators provide 24 x 7 x 365 coverage to detect incidents and to manage the impact and resolution.

What is your SLA policy for down time and outages?

The SLA for EC2 is provided on AWS Website: http://aws.amazon.com/ec2-sla/.

AWS will use commercially reasonable efforts to make Amazon EC2 available with an Annual Uptime Percentage of at least 99.95% during the Service Year. In the event Amazon EC2 does not meet the Annual Uptime Percentage commitment, you will be eligible to receive a Service Credit.

FAULT SEPARATION

How does AWS ensure redundancy across multiple data centers?

AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are typically physically separated within a metropolitan region and are in different flood plains. In addition to discrete uninterruptable power source (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single

points of failure. Availability Zones are all redundantly connected to multiple tier-1 transit providers.

Customers can select specific regions to meet location-dependent privacy and compliance requirements, such as the EU Data Privacy Directive. Data is not replicated between Regions unless proactively done so by customers, thus allowing customers with these types of data placement and privacy requirements the ability to establish compliant environments. It should be noted that all communications between Regions is across public Internet infrastructure. Appropriate encryption methods should be implemented to protect sensitive data.

Backups

How is data backed up within the Amazon Web Services Cloud Computing Platform?

Data stored in Amazon S3, Amazon SimpleDB, or Amazon Elastic Block Store is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. Amazon S3 and Amazon SimpleDB ensure object durability by storing objects multiple times across multiple Availability Zones on the initial write and then actively doing further replication in the event of device unavailability or detected bit-rot. Amazon EBS replication is stored within the same Availability Zone, not across multiple zones and therefore it is highly recommended that customers conduct regular snapshots to Amazon S3 in order to ensure long-term data durability AWS does not perform backups of data that are maintained on virtual disks attached to running instances on Amazon EC2.

Accellion does allow for its metadata to be backed up on a weekly basis. The backup can be pushed to the location of your choice.

ADDITIONAL INFORMATION

For further information please refer to the following resources:

Amazon Web Services

About Accellion

Accellion Secure Collaboration and File Transfer solutions are used by leading enterprise organizations including Procter & Gamble; Activision; Indiana University Health; Kaiser Permanente; Foley & Mansfield; Lovells; Bridgestone; Ogilvy & Mather; Harvard University; Guinness World Records; US Securities and Exchange Commission; and NASA.

For more information, please visit www.accellion.com or call +1 650-485-4300.

www.accellion.com **info@accellion.com**